FedCIRC

Practical Intrusion Detection Introduction

Sandy Sparks, FedCIRC-W

Rich Pethia, FedCIRC-E

Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

UCRL-MI-127241
CSTC 97-063

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

CIAC is the U.S. Department of Energy’s Computer Incident Advisory Capability. Established in 1989, shortly after the Internet Worm, CIAC provides various computer security services to employees and contractors of the DOE, such as:

- Incident Handling consulting
- Computer Security Information
- On-site Workshops
- White-hat Audits

CIAC is located at Lawrence Livermore National Laboratory and is a part of its Computer Security Technology Center. CIAC is also a founding member of FIRST, the Forum of Incident Response and Security Teams, a global organization established to foster cooperation and coordination among computer security teams worldwide.

Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the University of California, the United States Department of Energy, or the United States Government.

Other technical contributors

- Georgia Killcrece, FedCIRC-E

First, a word from our sponsor

- FedCIRC, a computer incident response capability for civilian federal agencies
- Established with seed money from the Government Innovative Technologies Services (GITS) Board
- To provide
  - Incident response
  - Incident prevention information
  - Assistance in establishing on-site incident handling capability
  - Vulnerability and incident trend information
- This seminar is an example of the services FedCIRC provides to its customers

During the next 2 days

FedCIRC will discuss:

- Today’s threats
- The role of intrusion detection
- Practical solutions to detection and monitoring with an emphasis on intrusion detection tools

Introduction

- Some basic definitions
- The state of intrusions today
- The importance of intrusion detection
- Intrusion indicators
- State of intrusion detection tools
- What about monitoring? Scott Charney, DOJ
- What role do policies and procedures play?

Glossary

First, we need a set of common definitions:

- A computer security incident is an adverse event in a computer system or network caused by a failure of a security mechanism, or an attempted or threatened breach of those mechanisms [Schultz90]
- An intrusion is defined as any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource [HLMS90]

Glossary (continued)

- Again, according to Webster, intrusion detection (ID) is the act of discovering or determining the existence, presence, or fact of (an intrusion)
- Intrusion detection is the methodology by which intrusions are detected (i.e., intrusion detection attempts to detect an intruder breaking into a system or a legitimate user misusing system resources)

For this seminar, intrusion detection is limited to:

Detecting, tracking and logging unauthorized activity on a computer system or computer network

Detecting and investigating anomalous activities that might be the result of an attempted intrusion or virus infection

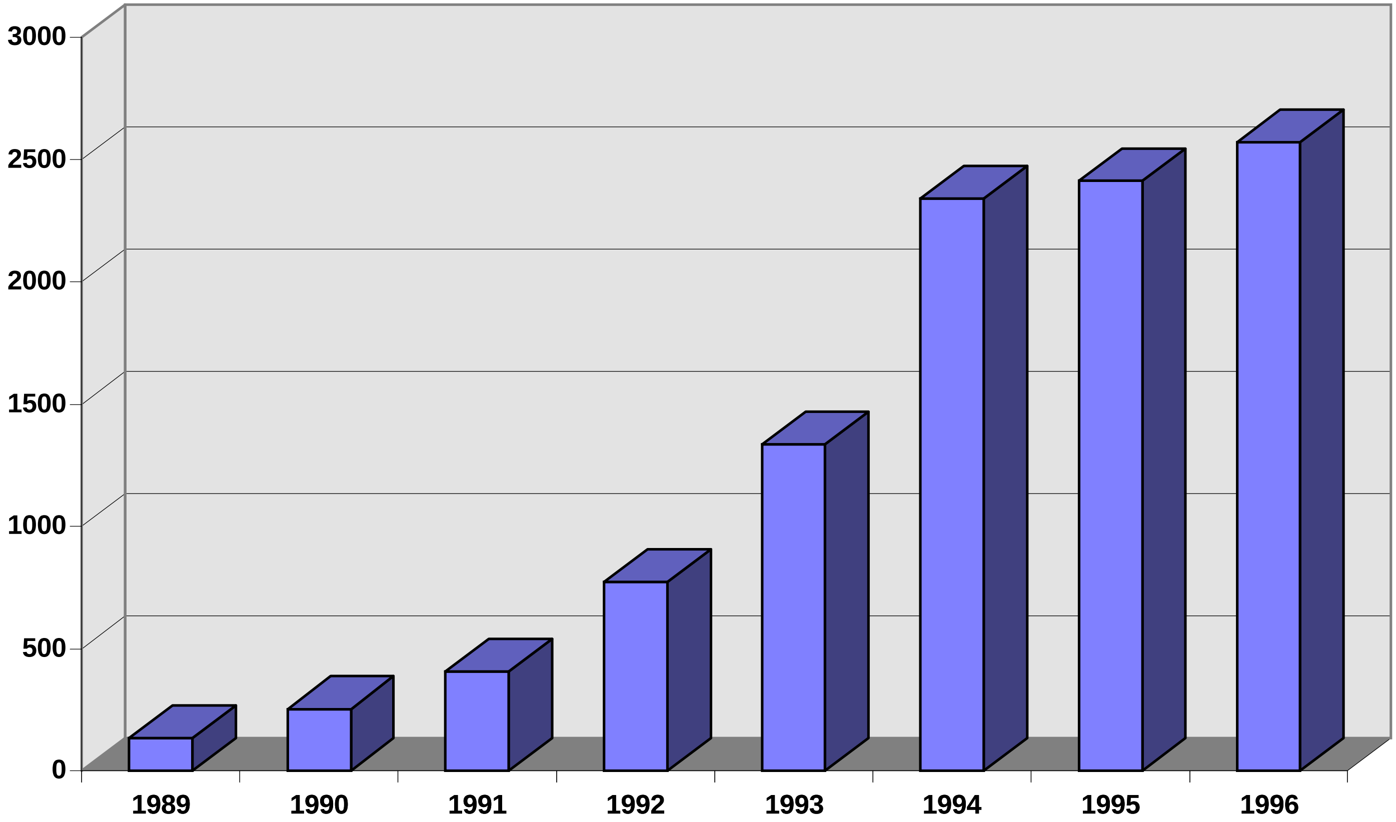
Purpose of this seminar

- Improve the ability of Federal Civilian Agencies to detect intrusions or intrusion attempts
  - Intrusions are on the rise
  - Many intrusions or intrusion attempts tend to go unnoticed
    - A good example is the DoD study from 1996
  - There are ways of detecting most of today’s intrusions and intrusion attempts
    - Tools, both public domain and commercial, can help

Purpose of this seminar

- The seminar will cover
  - Intrusion detection for
    - Unix-based, host-based
    - Networks
    - Non-Unix-based (Windows NT, Novell, Macintosh) intrusion detection
    - Viruses
  - Intrusion detection tools for the above
    - General descriptions as to OS, purpose, and availability
- Intrusion prevention and response are not covered

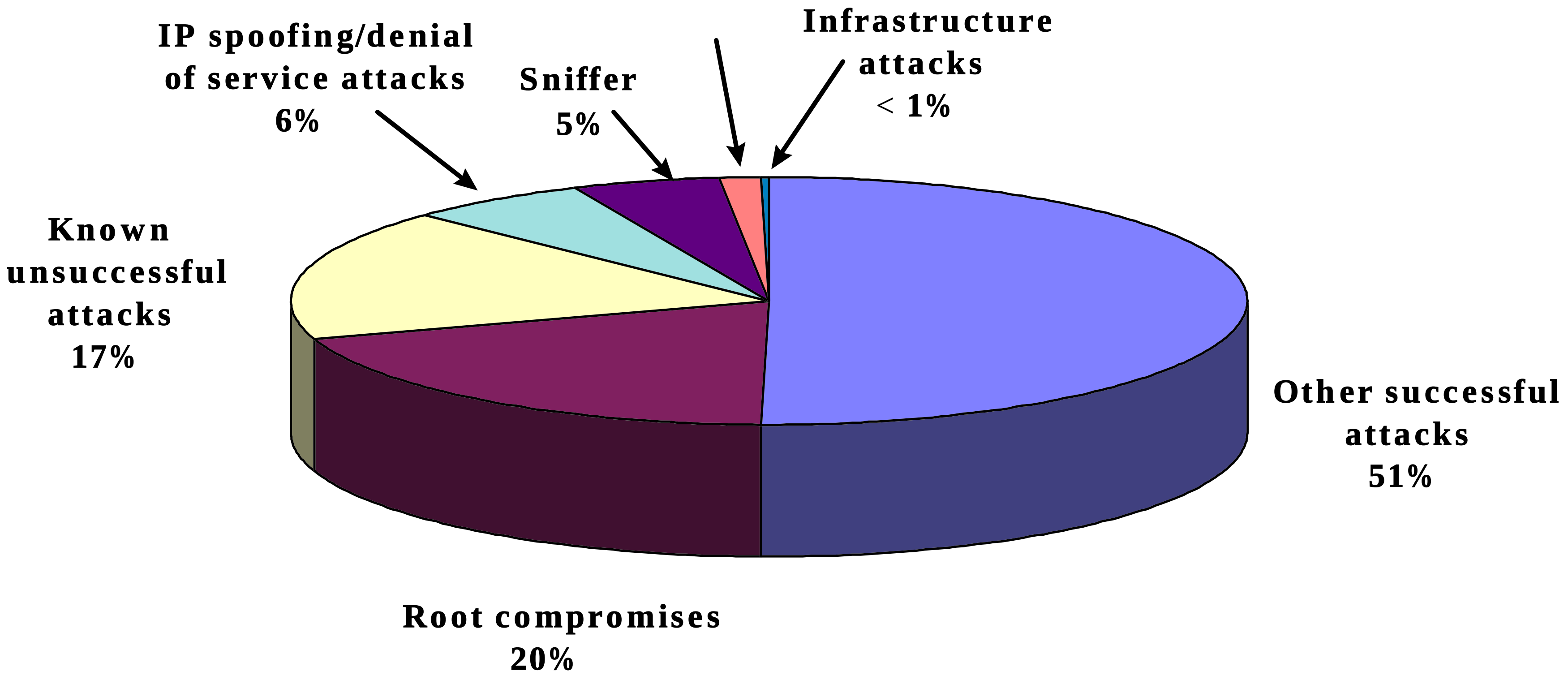
It is common knowledge that incidents are increasing



>10,000 Incidents Reported

(CERT/CC Statistics)

Incident types



1996 Percentage of incidents reported to CERT/CC

Other successful attacks category

- Include
  - Break-ins, Password cracking
  - Sendmail attacks
  - Misconfigured systems/Vulnerability exploited
  - Web abuse/Anon FTP abuse/Software piracy
  - Scans (ISS, NFS, NIS, etc.)
  - Social Engineering
  - Mail spamming/spoofing
  - Prank/Fraud issues

Unsuccessful attacks category

- Include
  - Probes or other failed attempts
    - telnet, rlogin, FTP, break-in attempts
  - Scans (ISS, NIS, NFS, etc.)
  - Sendmail attacks
  - Attempts to grab password
  - tftp probes

Comparison of 1996 to Recent Activity

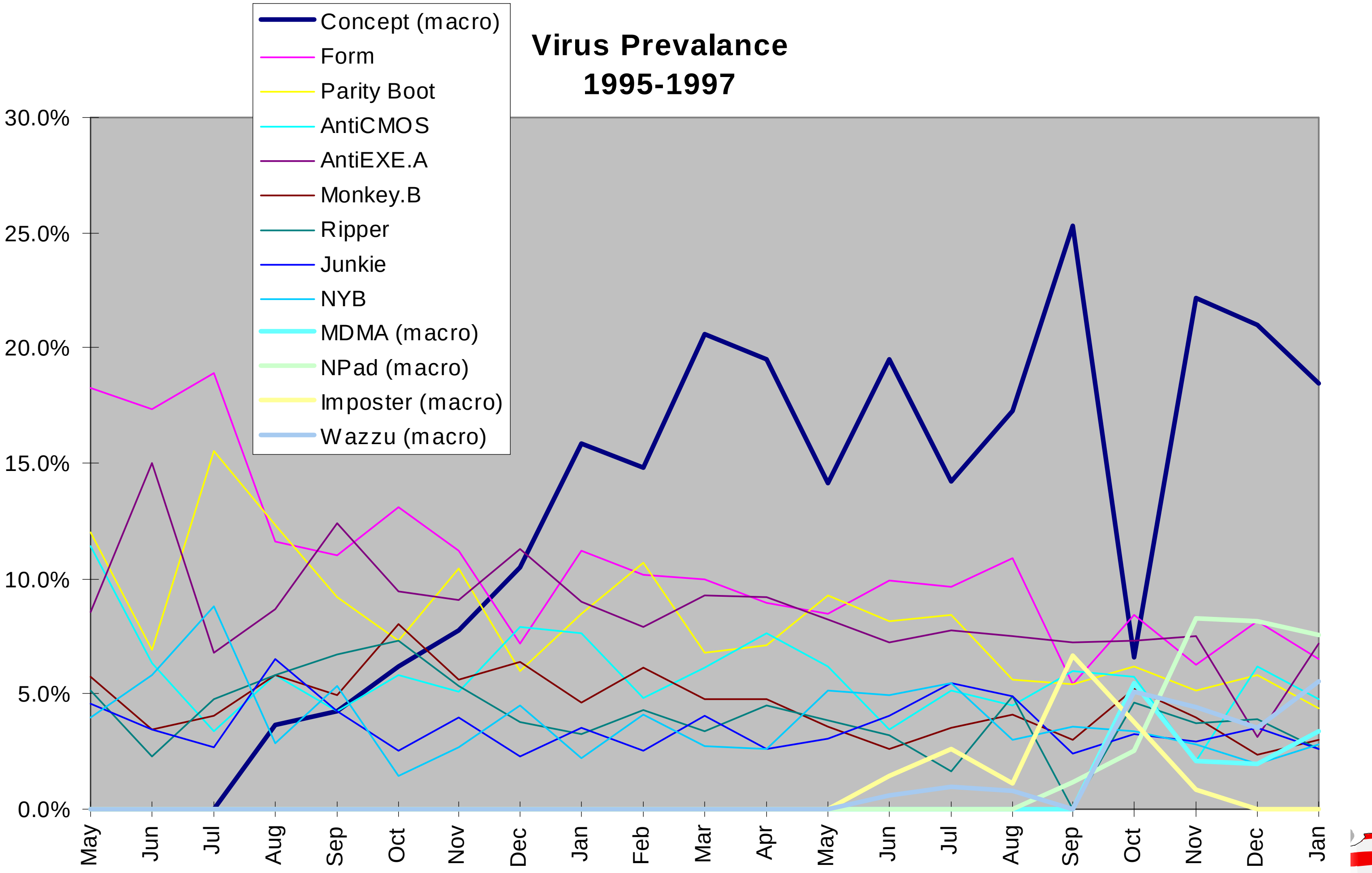
	1996	1997*
Other successful attacks	51%	24%
Root compromises	20	23
Unsuccessful attacks	17	32
IP spoofing/denial of service attacks	6	3
Sniffer	5	4
Information requests	1	0.1
Infrastructure attacks	0.2	0

*CERT/CC January through mid-March 97

Virus incidents are growing too

- In their *1996 Computer Virus Prevalence Survey,* The National Computer Security Association (NCSA) reports “virus incidents are some 3-5 fold more likely in early 1996 than early 1995”
- CIAC also continues to experience growth in the number of virus incidents
  - Virus incidents over the past two years are much more damaging than in the past

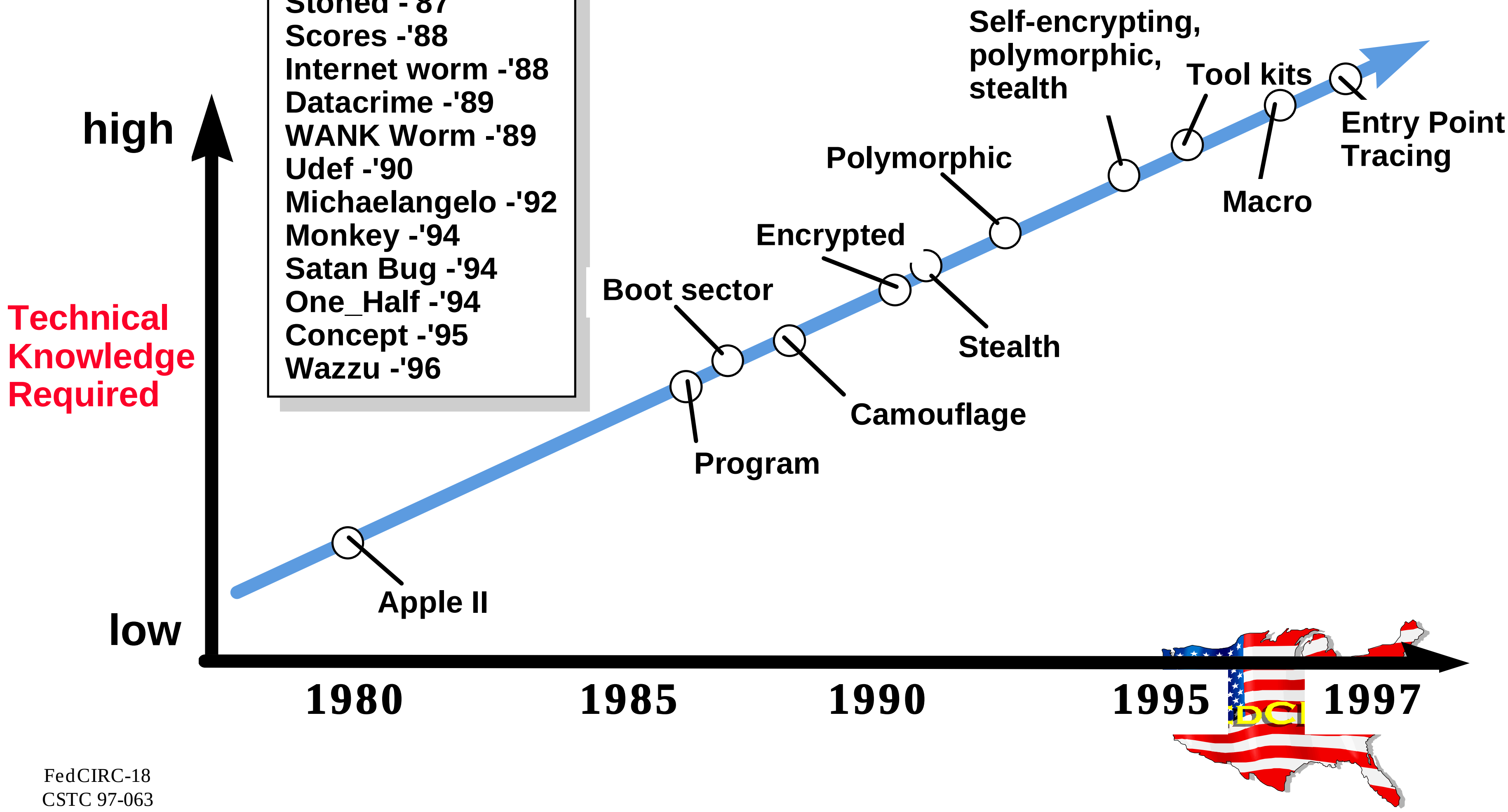
Virus prevalence chart



Source: Virus Bulletin, Virus Bulletin Limited, 1995-97

Virus incidents are becoming more damaging

Brain (PC) -'86
nVIR -'87
Jerusalem` -'87
Stoned -'87
Scores -'88
Internet worm -'88
Datacrime -'89
WANK Worm -'89
Udef -'90
Michaelangelo -'92
Monkey -'94
Satan Bug -'94
One_Half -'94
Concept -'95
Wazzu -'96

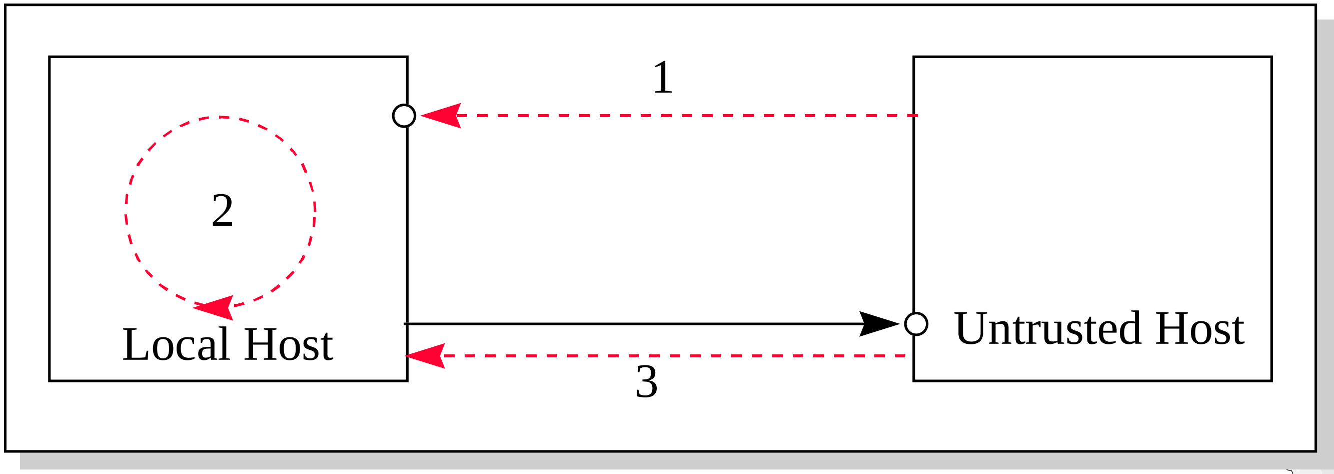


FedCIRC-18
CSTC 97-063

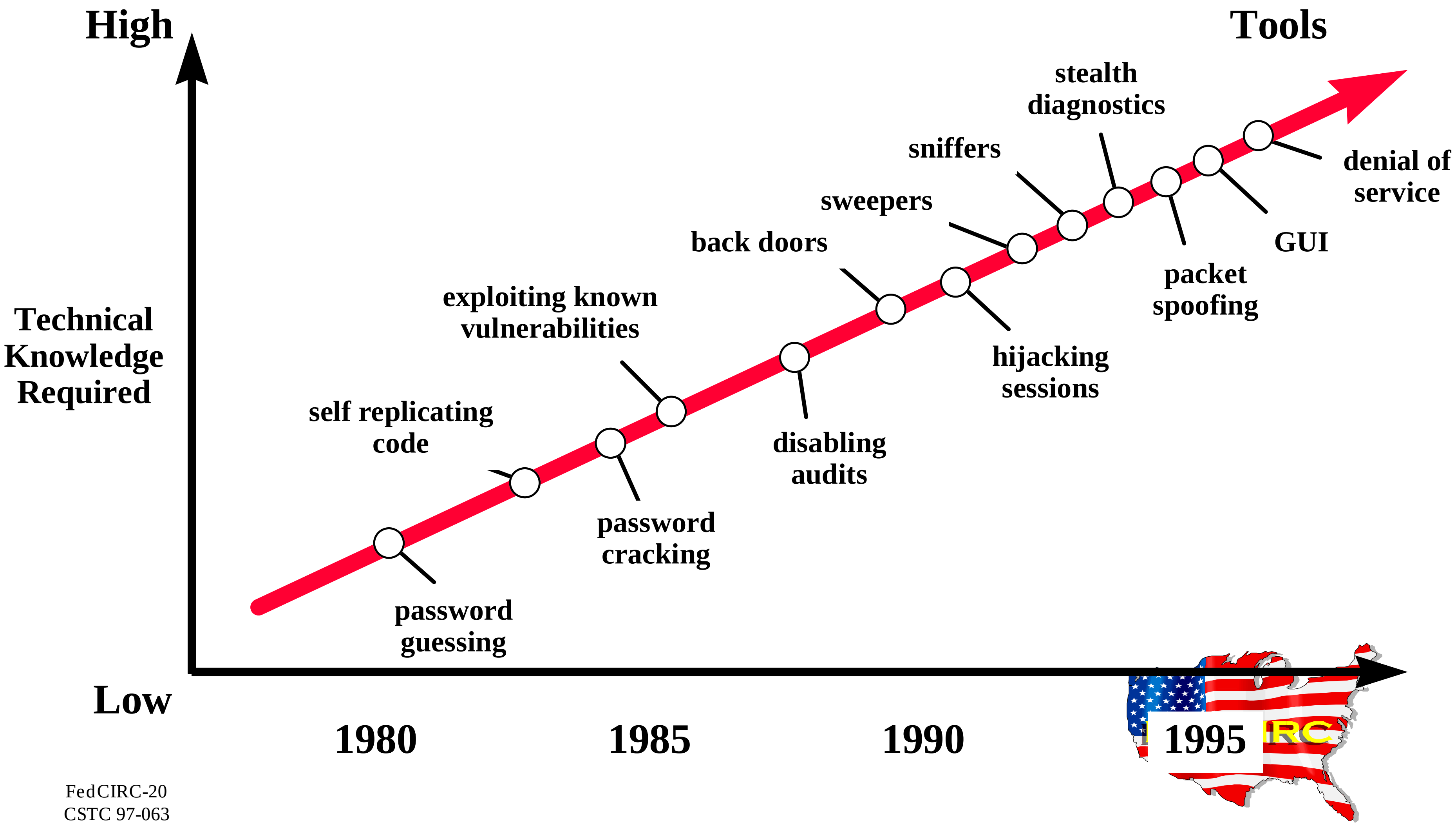
The changing threat environment

- Attack trends
  - Increased sophistication
    - More stealth; more automation
  - Changing motives and agenda
  - Changing environment

1. Attacks on network (and dial-up) services
2. Attacks against the local system such as virus attacks or non-privileged user attempting to gain privilege
3. Server attacks on client applications



Increased sophistication



High

Tools

Technical Knowledge Required

Low

password guessing

self replicating code

password cracking

exploiting known vulnerabilities

disabling audits

back doors

hijacking sessions

sweepers

sniffers

stealth diagnostics

packet spoofing

GUI

denial of service

1980

1985

1990

1995

Increasing automation

- Complex attacks are now automated
  - Sophistication for the Masses
  - 8lgm exploitation scripts
  - Rootkit
- Tedious vulnerability information collection can be automated
  - Internet Security Scanner (ISS)
  - Security Analysis Tool for Auditing Networks (SATAN)

8lgm Example

Check what root users are on the system:

```
>       % grep :0: /etc/passwd
```

●

We choose a user with UID 0, but without a /var/spool/mail/<username> file:

```
>       % ls -l /var/spool/mail/sysdiag
        /var/spool/mail/sysdiag not found
```

●

Execute mailscript. The user is sysdiag, the target file is /.rhosts, and the user to rsh to on success is root:

```
>       % chmod 700 mailscript
>       % ./mailscript sysdiag /.rhosts root
        mailscript: Warning, /.rhosts already exists,appending
        Sending mail to sysdiag
        We won the race, becoming root
        ./mailscript: 11051 Killed
        #
```

Changing operating environment

- Increasingly, our information assets reside on computer systems
- Information to use in perpetrating an intrusion is readily available
  - Mailing lists
  - World Wide Web (WWW) servers
  - Internet Relay Chat (IRC) lines, Bulletin Boards (BBS)
- Computer attacks are an economical way of gaining advantage
  - Politically
  - Economically

1996 CSI/FBI Computer Crime and Security survey

- “The results serve as a profound warning and a wake-up call”
  - 42% acknowledged they experienced unauthorized use of their computer systems within the last 12 months
  - These attacks included
    - brute force password guessing (13.9%)
    - scanning (15%)
    - denial of service (16.2%)
    - data diddling (15.5%)
  - The data diddling occurred primarily in financial institutions (21%) and medical institutions (36.8%)
  - According to the study, 50% of reported incidents occurred on internal nets and ~40% came via remote dial-in and Internet connections

Changes in intrusion profile

- 1988 Profile
  - Password Guessing - gain access to systems through easy to guess passwords
  - Widely known vulnerabilities - gain control of systems by exploiting vulnerabilities widely known and discussed by the technical community

Changes in intrusion profile (continued)

- 1995 Profile
  - Sniffer attacks - capturing data as it traverses the net
  - E-mail attacks - gaining system access through vulnerabilities in network service software
  - Network File System attacks - gaining data access through vulnerabilities in operating system software
  - Network Infrastructure attacks - denial of service through attacks on routers and name servers
  - IP Spoofing attacks - gaining system access by tunneling through firewalls

Changes in intrusion profile (continued)

- 1996 Profile
  - Exploiting passwords
  - Exploiting known vulnerabilities
  - Exploiting protocol flaws
  - Examining source files for new security flaws
  - Using ICMP attacks
  - Abusing anonymous FTP, web servers, email
  - Installing sniffer programs
  - IP source address spoofing
  - Denial of service attacks

Changes in intrusion profile (continued)

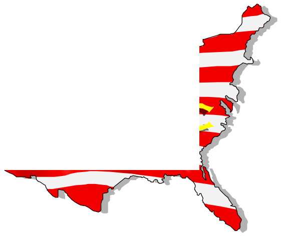
- Today
  - Many known vulnerabilities still being exploited even though patches available
  - Password cracking still produces results
  - Unix is still the OS of choice to exploit
  - At least one new vulnerability discovered per week
    - *Scriptors of Doom* targeting HP regularly
  - PC viruses abound - *macro* virus spreading
    - http://fedcirc.llnl.gov/viruses/

Changes in intrusion profile (continued)

- Today
  - Hoaxes developing lives of their own
    - Denial of Service attack in their own right
    - *Deeyenda, Good Times, Irina*
    - *http://ciac.llnl.gov/ciac/CIACHoaxes.html*
  - Trojan programs actively used - *rootkit*
  - Sniffers actively used and effective
    - Sniffer detectors are available for several OS
    - ftp://ciac.llnl.gov/pub/ciac/sectools/unix/sniffdetect
    - ftp://info.cert.org/pub/cert_advisories/CA-94:01.ongoing.network.monitoring.attacks

Changes in intrusion profile (continued)

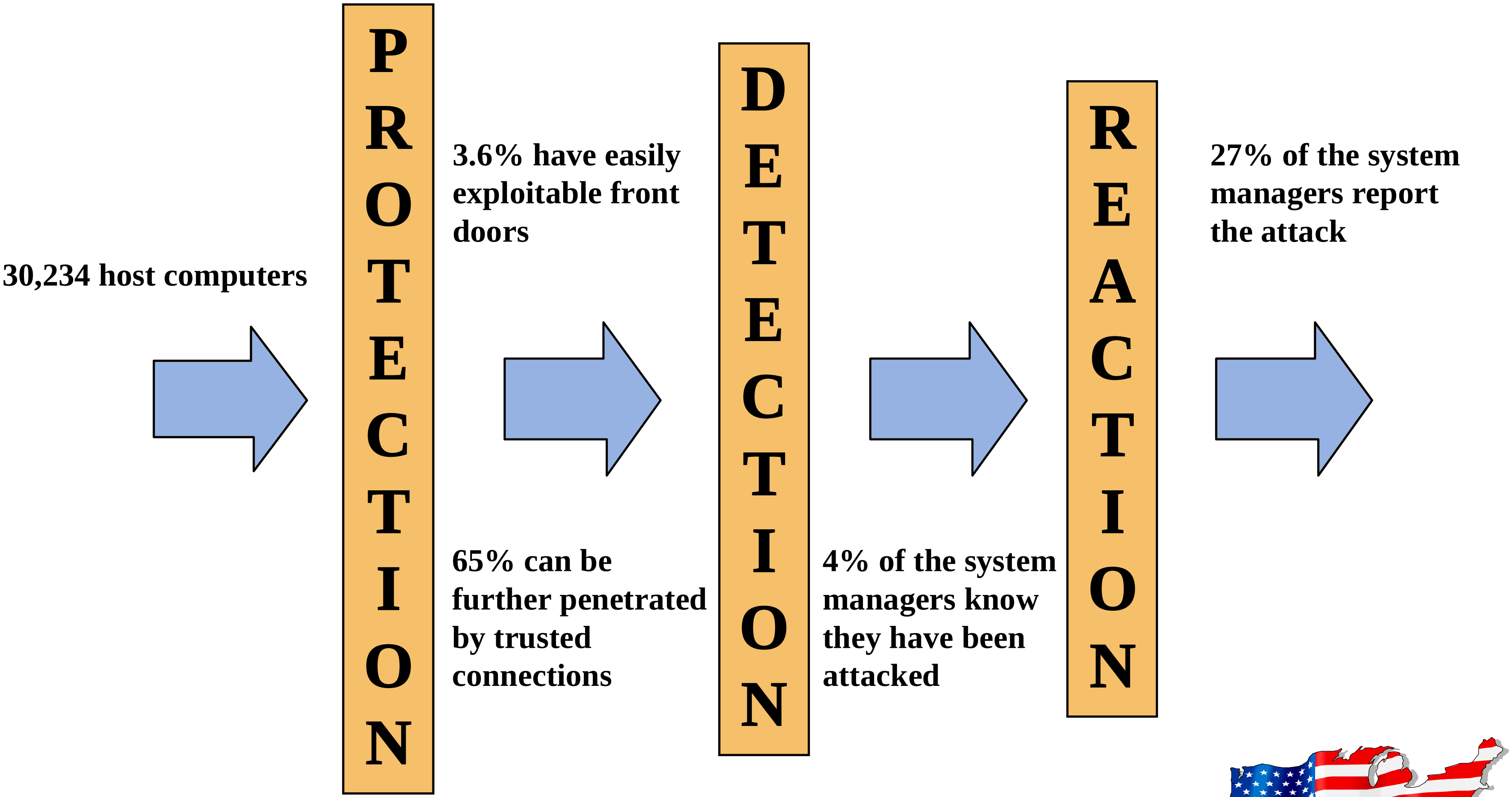
- Today
  - Increase in IP Spoofing attacks
    - Disallow source routing
    - Replace *rcp, rlogin, rsh* with *ssh*
    - ftp://info.cert.org/pub/cert_advisories/CA-95:01.IP.spoofing.attacks.and.hijacked.terminal.connections
  - Denial of Service attacks appearing
    - Internet Service Providers hit
      - ftp://info.cert.org/pub/cert_advisories/CA-96.01.UDP_service_denial
    - *SYN Flood* attack
      - ftp://info.cert.org/pub/cert_advisories/CA-96.21.tcp_syn_flooding
    - *Ping o' Death* attack
      - ftp://info.cert.org/pub/cert_advisories/CA-96.26.ping
      - http://ciac.llnl.gov/ciac/bulletins/h-12.shtml



Changes in intrusion profile (continued)

- **Today**
  - ***ssh*** **and** ***PGP*** **beginning to be used more**
  - **Web Home Pages being altered**
    - **DOJ, CIA, USAF, NASA**
    - **Mirror Site - http://www.skeeve.net/cia**
  - ***"Internet is now the fastest growing means for foreign governments and firms to gather information about U.S. businesses."***
    - **Source: National Counterintelligence Center**

However,
most intrusions go undetected



30,234 host computers

PROTECTION

3.6% have easily exploitable front doors

65% can be further penetrated by trusted connections

DETECTION

4% of the system managers know they have been attacked

REACTION

27% of the system managers report the attack

DoD's current experience in unclassified systems protection

Source: DISA

Intrusions are costly

- If you are fortunate enough to detect an intrusion, containing it and restoring your site back to normal operations is costly
  - A network-wide infection by the one-half virus cost a site 4000 lost hours at a cost of $90K (GS-11)
  - One site had its password file stolen and posted on an Internet bulletin board. They placed the dollar cost at $40K, but worse, they had to disconnect their site from the Internet for 87 hours while changing 10K compromised passwords
  - Cleanup from sniffer attacks have cost from $40-100K

Based on past CIAC data

Intrusion detection works

Cheswick and Bellovin in *Firewalls and Internet Security - Repelling the Wiley Hacker* reported:

100 times as many incidents were detected with high quality intrusion detection in place than without it!!!

So if it works, why . . .

- So if it works, why are intrusions not being detected as indicated in the DoD and other studies
  - The size of the audit records produced in a day of normal use in a typical Unix-based timesharing environment is on the order of 100,000 characters [Proctor94]
  - A skilled system administrator, reviewing this much data manually, would need up to 2 hours/system
  - An unskilled system administrator, would need double this time even if s/he knew what to look for and what to do
  - System administrators have other things to do than review audit logs, that is why intrusion detection tools and audit log reduction tools are so important

Generic intrusion indicators [NISTB]

- Activities that move a system from a “safe” state to an “unsafe” state
  - As in a virus infection
- Any “unauthorized” activity
- Activity that violates site policy
- Actions resulting in corruption/leakage/denial
- Unexplained anomalous behavior by a system
- A report from an intrusion detection tool such as an antivirus product

What are the basic steps to follow in detecting intrusions?

- Step 1. If you don’t have any installed intrusion detection tools, then you must understand the nature of intrusions in the area with which you are concerned
- Step 2. Look for the generic signs of intrusions in audit logs, in file systems, etc.
- Step 3. Act on your findings

Specific indications of intrusions

- A system alarm or similar indication from an intrusion detection tool
- Suspicious entries in system or network accounting
  - (e.g., a UNIX user obtains root access without going through the normal sequence necessary to obtain this access)
- Accounting discrepancies
  - (e.g., someone notices an 18-minute gap in the accounting log in which no entries whatsoever appear)
- Unsuccessful logon attempts

http://pokey.nswc.navy.mil/Docs/incident.indications.html

FEDCIRC

Specific indications of intrusions (continued)

- Unexplained, new user accounts
- Unexplained, new files or unfamiliar file names
- Unexplained modifications to file lengths and/or dates, especially in system executable files
- Unexplained attempts to write to system files or changes in system files
- Unexplained modification or deletion of data
- Denial of service or inability of one or more users to login to an account

http://pokey.nswc.navy.mil/Docs/incident.indications.html

Specific indications of intrusions (continued)

- System crashes
- Poor system performance
- Unauthorized operation of a program or sniffer device to capture network traffic
- "Door knob rattling"
  - (e.g., use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts)
- Unusual time of usage
  - (remember, more security incidents occur during non-working hours than any other time)

http://pokey.nswc.navy.mil/Docs/incident.indications.html

Specific indications of intrusions (continued)

- An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user
- Unusual usage patterns
  - e.g., programs are being compiled in the account of a user who does not know how to program

Although no single one of these typical symptoms of security incidents is generally by itself conclusive, observing one or more of these symptoms should prompt you to investigate events more closely. . .

http://pokey.nswc.navy.mil/Docs/incident.indications.html

Intrusion detection requires auditing [Lunt]

- Insures user accountability
- Has deterrent value
- Detects potential security violations
- Assists in gathering information if a legal case must be built
- Helps assess the extent of damage from a security incident

Intrusion detection activities are not without cost [Lunt]

- Someone must regularly review the output of your intrusion detection tools
- Someone must regularly review audit log files
- Someone must patch the holes used by insiders or outsides to compromise your systems
- A site-wide, up-to-date antivirus product must be made available and users required to use it

Intrusion detection tools [Lunt]

Attempt to:

- Detect a wide variety of intrusion types
- Provide for real-time detection
- Display and interpret current and past events
- Be easy to use
- Adapt to a diverse computing environment
- Present believable findings
  - Low number of false positives (normal activities flagged as an intrusion)
  - Low number of false negatives (intrusion activities that are presented as normal)

State of intrusion detection tools [NTBID&R report]

- Improved over the last 10 years
- Attempting to add
  - Artificial intelligence to reduce the need for experts to review logs
  - Cross-platform analysis for today’s heterogeneous environment
  - Networked-based and distributed instead of system specific
  - Improved audit reduction
  - Automated response
  - Affordable
- One of today’s biggest problems is
  - Audit log data reduction and review, both in real-time and after the fact

Intrusion detection equates to monitoring . . .

. . . of computer and network usage which now becomes a privacy issue as well as a policy issue

DOJ Presentation

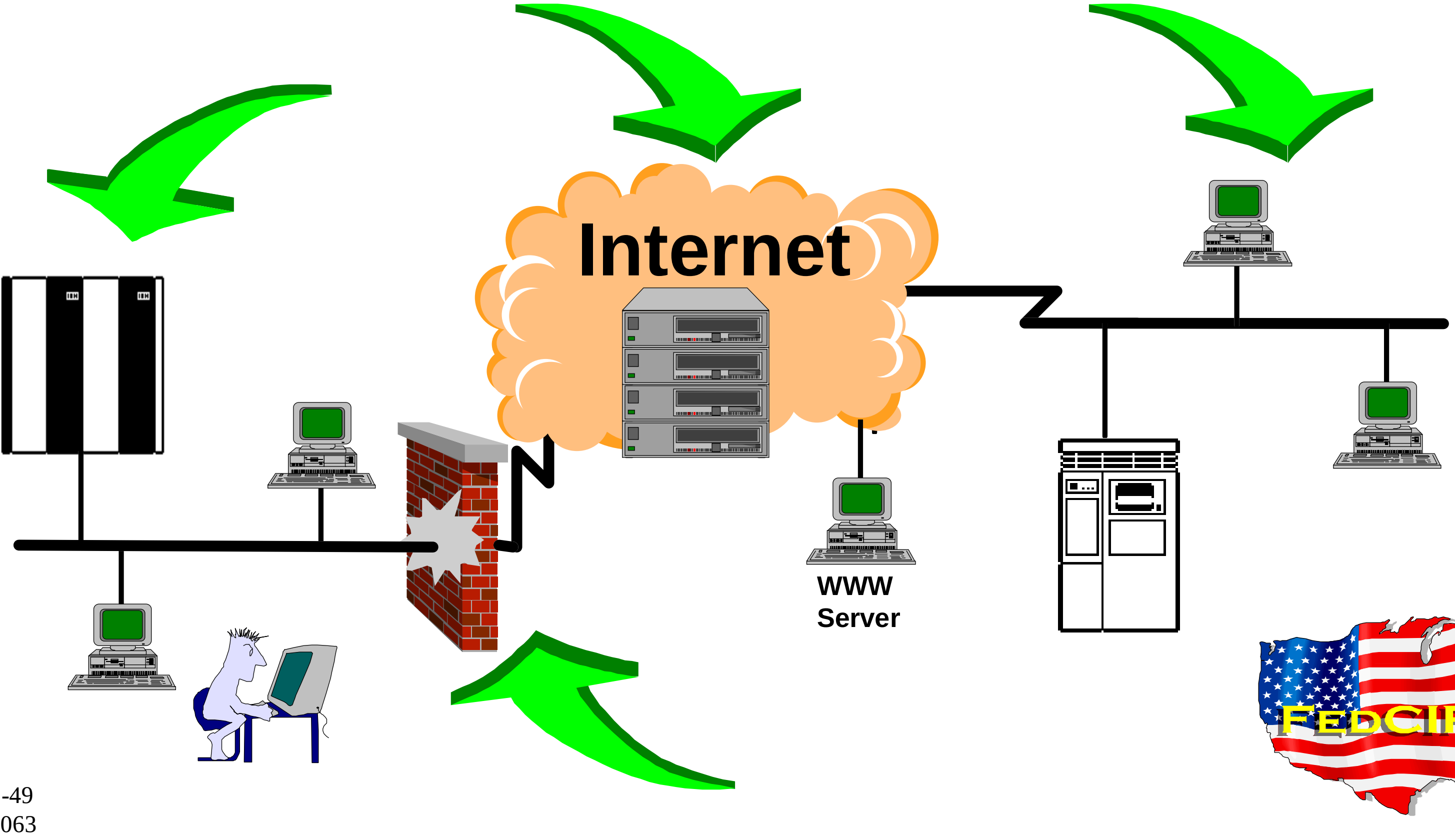
- Guest Speaker: Scott Charney

What role do policies and procedures play?

- What to do when an intrusion is discovered?
- Who is notified? Who does the notifying?
- Requirements for use of antivirus software and other intrusion detection software?
- Requirements for review of audit logs?
- What can employees expect to be monitored?
  - Files
  - E-mail
  - Net usage
  - Internal nets
  - External nets

Where do intrusions occur?

- On Internet infrastructure servers
- On network servers
- On multi-user hosts
- On firewalls
- On public web servers
- At individual workstations



Now let’s move on to the technical sessions on ID

- **Each session will provide**
  - Information about the tools available for specific environments and to meet specific intrusion detection goals
  - Pointers and references
- **As you listen to each session, keep these things in mind**

Where to use ID tools to obtain maximum benefit?

- Use of tools depends
  - On the layout of a site's network environment
  - How it is connected to the Internet
  - Whether or not the organization intends to provide publicly accessible services
- Within the framework of this workshop, suggestions/guidance will be provided to improve your implementation of intrusion detection tools

How do you interpret the data collected by ID tools?

- Each tool will give information about certain aspects of your network and host operations
- Using these information sources, you will attempt to identify
  - Suspicious,
  - Unauthorized,
  - Or other abnormal behavior of your systems and networks

What doesn't intrusion detection do?

- Doesn't solve the problem
- Doesn't fix the problem
- May not always tell you who/how the attack occurred
- May not tell you the motive of the attacker

Bibliography

- [Lunt] T. Lunt. *Intrusion Detection* presented to San Francisco Chapter of the IEEE Computer Society, November, 1994
- [NISTB] National Info-Sec Technical Baseline Report: *Intrusion Detection and Response.* Lawrence Livermore National Laboratory, Sandia National Laboratory, October, 1996
- [HLMS90] R. Heady, G. Luger, A. Maccabe, and M. Servilla. *The Architecture of a Network Level Intrusion Detection System.* Technical report, Department of Computer Science, University of New Mexico, August 1990
- [Proctor94] P. Proctor, *A Computer Misuse Detection System*, 1994.
- [Schultz90] *Responding to Computer Security Incidents: Guidelines for Incident Handling*, Eugene Schultz, David Brown, Tom Longstaff, July 23, 1990, UCRL-ID-104689